U.S. Department of Transportation
Federal Aviation Administration

Subject:	The Role of Maintenance Computers in Exposure Time Assumptions For Quantitative Safety Analyses	Date:	Feb. 22, 1995
From:	Transport Airplane Directorate, ANM-100	Reply to Attn. of:	Policy Ltr. TAD-95-001

To: Manager, Small Airplane Directorate, ACE-100
Manager, Aircraft Engineering Division, AIR-100
Manager, Engine and Propeller Directorate, ANE-100
Manager, Seattle Aircraft Certification Office, ANM-100S
Manager, Los Angeles Aircraft Certification, ANM-100L
Manager, Rotorcraft Directorate, ASW-100

The trend toward complex fault-tolerant, flight-critical systems in transport airplane designs has led to an increased reliance on quantitative safety assessments, to assure compliance with §25.1309(b)(1), §25.901(c), §25.903(b), and other "fail-safe" regulations. Since any safety analysis is only as accurate as the assumptions, data, and analytical techniques utilized, the validity of each of these factors must be formally justified to a level appropriate for the criticality of the analysis. In recent transport programs, applicants have presented quantitative systems safety assessments of catastrophic failure conditions where the ability to detect, isolate, and eliminate faults prior to the assumed exposure times was dependent on installed equipment categorized as "nonessential" (e.g., central maintenance computers). This may be appropriate provided this equipment meets the following criteria:

a. The equipment is shown to comply with §25.1301(d) by:

(1) A specific system certification test demonstration of the maintenance functions for which credit is taken. [1]

(2) Development and certification of any software which could affect the availability or accuracy of the subject maintenance functions in accordance with RTCA/DO178B standards.[2]

b. The effects of hardware availability and failure modes are predicted and accounted for in the subject safety assessment (e.g., if the equipment is assumed to detect a particular failure, then an appropriate percentage of these failures should be assumed to be "made latent" by anticipated failures in the detection equipment).

If these criteria are not met, then no credit should be given for the installed equipment in any systems safety assessment of catastrophic or hazardous failure conditions.

Please bring this information to the attention of the transport category airplane manufacturers and the appropriate designated engineering representative in your official area of responsibility.

Sincerely,

Ronald T. Wojnar
Manager, Transport Airplane Directorate,
Aircraft Certification Service

[1] This demonstration can be done as an end-to-end fault insertion test on the complete system, or be derived from component test results. If the latter approach is selected, adequate interface validation must be provided.

[2] The actual software substantiation required should be agreed to with the certifying office early in the project and be made part of the approved certification plan. The software level selected should be based on the potential consequences of errors. Normally, software affecting the ability to detect, isolate, and eliminate faults, which could contribute to or cause a hazardous or catastrophic failure condition, should be developed to level C or better. However, in circumstances where the criticality of software errors is minimal, but some credit for the ability is needed, validation to Level D of RTCA DO-178B may be acceptable, provided this is supplemented with appropriate software reliability testing/analysis of the subject functions. The software reliability should be shown to be at least one order of magnitude better than what is essential to support the required event probabilities. (Note: Current software reliability models are only reasonable for probability predictions > $1X\ 10^{-5}$.)